AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Previously Presented) The method as claimed in claim 30, in which the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means.

5. (Previously Presented) The method as claimed in claim 4, in which the decoder is associated with a portable security module used to store transmission access control keys (KO(NS), KO'(Op1, NS) etc.) used to decrypt the transmitted encrypted information.

6. (Previously Presented) The method as claimed in claim 5, in which at least one of the recording encryption key (E (NE)) and the recording transport key (RT (A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (KO(NS), KO' (Opl, NS) etc.) function in accordance with a second encryption algorithm (CA).

7. (Previously Presented) The method as claimed in claim 30, which the recording transport key (RT (A)) is generated at a central recording authorization unit and a copy of this key communicated to the recording means.

8. (Previously Presented) The method as claimed in claim 7, in which the recording transport key (RT (A)) is encrypted by a further encryption key (KO(NSIM)) prior to being communicated to the recording means.

9. (Previously Presented) The method as claimed in claim 30, in which a central access control system communicates transmission access control keys (KO (NS), KO'(Op1, NS) etc.) to the recording means.

10. (Previously Presented) The method as claimed in claim 9, in which the transmission access control keys (KO(NS), KO' (Opl, NS) etc.) are communicated to a portable security module associated with the recording means.

11. (Previously Presented) The method as claimed in claim 9, in which the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO'(Opl, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium.

12. (Previously Presented) The method as claimed in claim 9, in which the central access control system encrypts the broadcast access control keys (KO(NS), KO' (Opl, NS) etc.) by a further encryption key (KO (NSIM)) prior to their communication to the recording means.

13. (Previously Presented) The method as claimed in claim 9, in which the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO(NS), KO'(Opl, NS) etc.), the request of authentification by the recording means using a key (KO(NSIM)) unique to that recording means.

14. (Previously Presented) The method as claimed in claim 30, using a decoder means and associated security module and a recording means and associated security module and in which a copy of the recording transport key (RT (A)) is stored in at least one of the security module associated with the decoder means and the security module associated with the recording means.

15. (Previously Presented) The method as claimed in claim 14, in which the recording transport key (RT (A)) is generated by either the recording security module or decoder security module and communicated to the other security module.

16. (Previously Presented) The method as claimed in claim 15, in which the recording transport key (RT (A)) is encrypted before communication to the other security module and decrypted by a key unique (KO(NS)) to that other security module.

17. (Previously Presented) The method as claimed in claim 16, in which the decoder security module and recording security module carry out a mutual authorization process, the unique

decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorization.

18. (Previously Presented) The method as claimed in claim 17, in which the mutual authorization step is carried out using, inter alia, an audience key Kl (C) known to both security modules.

19. (Previously Presented) The method as claimed in claim 14, in which the decoder security module possesses transmission access control keys (KO(NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3 (NSIM)) re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)).

20. (Previously Presented) The method as claimed in claim 19, in which the session key (K3 (NSIM)) is generated by one of the decoder security module and recording means security module and communicated to the other module in encrypted form using an encryption key (KO (NS)) uniquely decryptable by other security module.

21.-29. (Cancelled)

30. (Currently Amended) A method of recording transmitted digital data, comprising:

receiving the transmitted digital data comprising scrambled data and encrypted transmitted digital information;

decrypting the encrypted transmitted digital information to obtain transmitted digital information, wherein the transmitted digital information comprises a control word, and wherein the control word is used to descramble the scrambled data;

re-encrypting the transmitted digital information ~~of the transmitted digital data by~~ using a recording encryption key~~, wherein the transmitted digital information comprises a control word~~;

storing the re-encrypted transmitted digital information and the scrambled data by a recording means on a recording support medium;

encrypting the recording encryption key by a recording transport key; and

storing the encrypted recording encryption key to the recording support medium,

wherein at least one of the recording encryption key and the recording transport key is stored on a portable security module associated with the recording means.

31. (Currently Amended) A system for recording transmitted digital data, comprising:

a receiver/decoder for at least:

receiving the ~~encrypted~~ transmitted digital data, wherein the ~~encrypted~~ transmitted digital data comprises scrambled data and encrypted transmitted digital information, wherein the encrypted transmitted digital information comprises a control word used to descramble the scrambled data;[[, and]]

decrypting the encrypted transmitted digital information to obtain the control word,

wherein the transmitted digital data is re-encrypted using a recording encryption key; and

a recording means for recording the re-encrypted transmitted digital information [[data]] to a recording support medium, along with an encrypted recording encryption key, wherein the recording encryption key is encrypted via a recording transport key to obtain the encrypted recorded encryption key.

32. (Previously Presented) The system as claimed in claim 31, further comprising:

a decoder means and associated security module adapted to store a copy of the recording transport key (RT(A)).

33. (Previously Presented) The system as claimed in claim 32, in which the security module associated with the decoder means is adapted to descramble transmitted information using one or more transmission access keys prior to re-encryption by a session key for subsequent communication to the recording means.

34. (Currently Amended) A system for recording transmitted digital data comprising scrambled data and encrypted transmitted digital information, comprising:

a recording support medium configured to store the encrypted transmitted digital information [[data]], and an encrypted recording encryption key, wherein the encrypted transmitted digital information [[data]] comprises a control word used

to descramble the scrambled data, wherein the transmitted digital information [[data]] is re-encrypted using a recording encryption key, and wherein the encrypted recording encryption key is encrypted using a recording transport key; and

a portable security module configured to store at least one of the recording encryption key and the recording transport key.

35. (Currently Amended) A recording support medium, comprising:

transmitted digital data, wherein the transmitted digital data comprises scrambled data and encrypted transmitted digital information, wherein the encrypted transmitted digital information comprises a control word used to descramble the scrambled data, and wherein the encrypted transmitted digital information is decrypted to obtain the control word,

wherein the decrypted transmitted digital information is re-encrypted using a recording encryption key~~, and wherein the transmitted digital data comprises a control word~~; and

an encrypted recording encryption key, wherein the encrypted recording encryption key is encrypted using a recording transport key.

36. (Currently Amended) A receiver/decoder used in a conditional access digital television system, comprising:

means for receiving ~~encrypted~~ transmitted digital data comprising scrambled data and encrypted transmitted digital information, wherein the encrypted transmitted digital information [[data]] comprises a control word used to descramble the scrambled data; and

means for decrypting the encrypted transmitted digital information to obtain the control word;

wherein the transmitted digital data is re-encrypted using a recording encryption key,

wherein the recording encryption key is encrypted via a recording transport key to obtain an encrypted recorded encryption key, and

wherein the receiver/decoder is operatively connected to a recording means for recording the re-encrypted transmitted digital information [[data]] and the encrypted recording encryption key to a recording support medium.